

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Kevin Zilka, reg. no. 41,429 on May 28, 2009.

3. The claims have been amended as follows:

a. Replace claim 1 to read as of the following,

In Claim 1,

1. (Currently Amended) A method of capturing and selectively analyzing data frames transmitted between stations in a communications network utilizing tunneling protocols, comprising:
establishing a connection with a communications network;
receiving, in real-time, data frames transmitted in the communications network, wherein the data frames are communicated utilizing tunneling; and

analyzing the data frames that are communicated utilizing the tunneling;
wherein the analyzing is conditionally performed for one or more types of tunnels associated with the tunneling based on user input;
wherein multiple objects generated by a plurality of protocol interpreters are linked to logically portray a relationship between endpoints of a tunnel and stations conversing inside the tunnel;
wherein byte counts distinguish between the stations conversing inside the tunnel and the endpoints of the tunnel.

- b. Replace claim 14 to read as of the following,

In Claim 14,

14. (Currently Amended) A computer program product embodied on a computer readable medium, comprising:
computer code for establishing a connection with a communications network;
computer code for receiving, in real-time, data frames transmitted in the communications network, wherein the data frames are communicated utilizing tunneling; and
computer code for analyzing the data frames that are communicated utilizing the tunneling;
wherein the computer program product is operable such that the analyzing is conditionally performed for one or more types of tunnels associated with the tunneling based on user input;

wherein the computer program product is operable such that multiple objects generated by a plurality of protocol interpreters are linked to logically portray a relationship between endpoints of a tunnel and stations conversing inside the tunnel;

wherein the computer program product is operable such that byte counts distinguish between the stations conversing inside the tunnel and the endpoints of the tunnel.

- c. Replace claim 28 to read as of the following,

In Claim 28,

28. (Currently Amended) A computer-implemented system, comprising:

a microprocessor;

a network analyzer coupled to a communications network for receiving, in real-time, data frames transmitted in the communications network,

the data frames being communicated utilizing tunneling, wherein the system is operable such that the data frames that are communicated utilizing the tunneling are analyzed, the analysis conditionally performed for one or more types of tunnels associated with the tunneling based on user input,

wherein the system is operable such that multiple objects generated by a plurality of protocol interpreters are linked to logically portray a relationship between endpoints of a tunnel and

stations conversing inside the tunnel; wherein the system is operable such that byte counts distinguish between the stations conversing inside the tunnel and the endpoints of the tunnel.

- d. Cancel claim 29 to read as of the following,

29. (Canceled).

- e. Cancel claim 34 to read as of the following,

34. (Canceled).

Reason for Allowance

5. The following is an examiner's statement of reasons for allowance: None of the prior arts of records teach or suggest in combination features of receiving, in real-time, data frames transmitted in the communications network, wherein the data frames are communicated utilizing tunneling, analyzing the data frames that are communicated utilizing the tunneling, wherein the analyzing is conditionally performed for one or more types of tunnels associated with the tunneling based on user input, wherein multiple objects generated by a plurality of protocol interpreters are linked to logically portray a relationship between endpoints of a tunnel and stations conversing inside the tunnel, wherein byte counts distinguish between the stations

conversing inside the tunnel and the endpoints of the tunnel. None of the prior arts of records teach or suggest the features above in combination with independent claims 1, 14 and 28.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip C Lee whose telephone number is (571)272-3967. The examiner can normally be reached on 8 AM TO 5:30 PM Monday to Thursday and every other Friday. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Firmin Backer can be reached on (571) 272-6703. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Philip C Lee/

Primary Examiner, Art Unit 2448